Report on

A Framework for International Cyber Stability

International Security Advisory Board

July 2, 2014

Disclaimer

This is a report of the International Security Advisory Board (ISAB), a Federal Advisory Committee established to provide the Department of State with a continuing source of independent insight, advice and innovation on scientific, military, diplomatic, political, and public diplomacy aspects of arms control, disarmament, international security, and nonproliferation. The views expressed herein do not represent official positions or policies of the Department of State or any other entity of the United States Government.

While all ISAB members have approved this report and its recommendations, and agree they merit consideration by policy-makers, some members may not subscribe to the particular wording on every point.

United States Department of State

Washington, D.C. 20520

July 2, 2014

MEMORANDUM FOR UNDER SECRETARY GOTTEMOELLER

SUBJECT: Final Report of the International Security Advisory Board (ISAB) on A Framework for International Cyber Stability

I am forwarding herewith the ISAB's report on a Framework for International Cyber Stability. The report responds to your request of July 17, 2013, that the Board undertake a study on a potential architecture for enhanced international cooperation in promoting a peaceful, secure, and open cyberspace environment. The report was drafted by members of a Study Group chaired by General Montgomery Meigs (USA, Ret.). It was reviewed by all ISAB members and unanimously approved by July 1, 2014.

The report aims at outlining a framework for international cyber stability. To do so, the report first describes existing and potential threats in cyberspace, realities associated with cyberspace that must be taken into account, and the role of deterrence in enhancing cyber stability. The report then offers a number of recommendations for the Department of State to undertake or support.

The ISAB advocates building on areas of consensus while exploring norms that relate to core U.S. values, using a two-tier approach: both bilateral dialogues and discussions at the multilateral level. Eventually, bilateral norms could be integrated into broader alliances, treaties and agreements. The goal would be to establish a broad multinational cooperative response mechanism to promote cyber stability. The report emphasizes engaging and partnering with the business community, since most cyber infrastructure and expertise lie in the private sector.

We encourage you to consider all of the report's recommendations carefully. The Board stands ready to brief you and other members of the Administration on the report.

Hon. Gary Hart
Chairman
International Security Advisory Board

This page intentionally blank

INTERNATIONAL SECURITY ADVISORY BOARD

Report on

A Framework for International Cyber Stability

TABLE OF CONTENTS

This page intentionally blank

Report on
A Framework for International Cyber Stability

Executive Summary

This report aims at outlining a framework for international cyber stability. Cyber stability would enhance continuity of relations between nations in the face of attack or exploitation through cyber means.

Since current international law is not yet well developed in the cyber realm, we propose that the United States articulate norms consistent with existing international law and U.S. values, while recognizing the uncertainties surrounding cyber activities. As the United States anticipates a response to all consequences of a cyber attack on itself, allies or vital interests, in order to limit unintended escalation the United States should set rigorous rules of engagement for military and civilian organizations for responding to significant attacks using cyber means.

Cyberspace is not defined geographically and our allies have yet to agree on norms for behavior within it. The ISAB supports a two-tier approach for building consensus on future norms and potential treaty obligations: continuing discussions at the multilateral level and pursuing vigorous bilateral dialogues with the goal of establishing mutually compatible norms and obligations. Eventually, bilateral norms could be integrated into broader alliances, treaties and agreements.

We advocate building on areas of consensus while exploring norms that relate to core U.S. values. For example, the principle of freedom of speech in cyberspace requires careful consideration in the light of the capability for authentication of messages and the fact that some speech is criminal and should not be protected. The power of the Internet lies in its openness, which must be balanced against, for instance, the need for resilience under attack, protection of privacy, and attribution.

Since most cyber infrastructure and expertise lie in the private sector, we propose establishing public-private partnerships. These partnerships would:

- identify norms for U.S. actions in cyberspace that the private sector could embrace;
- discuss the consequences of these actions;
- encourage best practices internationally;
- assist with creating international cooperative arrangements to share information on cyber attacks and responses.

The goal would be to establish a multinational cooperative response mechanism, which would promote confidence in the ability to sustain cyber stability.

Report on
A Framework for International Cyber Stability

Study Purpose: Recommend to the Department of State a framework and actions to gain enhanced international cooperation in promoting a peaceful, secure, and open environment in cyberspace.

Thesis: The growing understanding that the benefits and risks of cyberspace affect all nations and societies creates an opportunity to advance significantly international dialogue to define normative behaviors that will maintain and improve cyber stability.

A stable international cyberspace can be defined as an environment where all participants can positively and dependably enjoy its benefits, where there are incentives for cooperation and avoidance of conflict, and where disincentives for engaging in malicious cyber activity apply. A stable cyber framework has geopolitical, economic, technological, and legal elements. For the State Department, this framework requires the following:

- Understanding its risks, delineating its fundamental operating principles, and developing corresponding international norms and associated behaviors among states, while recognizing and encouraging the essential participation of non-governmental entities, especially the business community and within that community especially entities involved in the resilience of our infrastructure, sustaining persistent levels of service, and the national capability to attribute, deter and respond.

- Norms for behavior in this environment should foster attribution of and appropriate responses to attacks, including legal redress under national and international law in support of deterrence and de-escalation of cyber attacks as well as mitigation or restitution.

Framework for Analysis – The Threat:

Our immediate challenge in cyberspace derives from the combined impact of the accelerating evolution of capabilities in information technology, the inter-connectivity it enables, and the consequent ability of states and non-state organizations and actors to do both harm and good. The pervasive interconnected and complex nature of cyberspace makes it difficult to assess the interests of nations, the bounds of the problems, and the strategy for issues like attribution, recovery and reconstitution of systems after an event.

The risk landscape involves both technical and non-technical threats. Technical threats can significantly damage government systems and critical infrastructure, the confidentiality and integrity of government and private sector data, and individual identity. The continuing acceleration of productivity in information technology generates a profusion of "technically sweet" applications that proliferate at scale as popular demand explodes. Inherent in each application lies the opportunity for a diversity of actions, from nation-states to fourteen year olds, to manipulate the new "app" in ways never anticipated by the inventor. Threats are particularly concerning to countries with a high degree of dependency on cyber infrastructure, including the United States, where the risks are massive and possibly existential. But threats to the Internet as we know it also arise from non-technical factors such as international pressure to change Internet governance, to increase "national sovereignty" over Internet use and data, and other differences between states in political cultures and values.

A key element of cyber stability – trust – supports confidence among players that each will adhere to rules of the road in accordance with international standards, conventions, law, or consensus best practice, and that all can have reasonable confidence that the Internet will function as expected. The ability of the United States to make progress in diplomatic efforts to improve international cyber stability rests on enhancing and maintaining – even expanding – the good reputation of the United States and international trust in the USG, the U.S. cyber industry, U.S.-supported institutions and the best practices they recommend. Our effectiveness in this area has suffered from recent disclosures and exaggerated reports about intelligence collection activities. Success with all but the most like-

minded nations and institutions will depend on treading lightly if persistently, as well as allowing and enabling other parties to take the leadership role on various issues.

There are three prominent cyber threat vectors. The supply chain presents the first. The National Academies of Sciences highlighted in a recent report that "faulty, counterfeit, or deliberately vulnerable components" could be introduced into the supply chain[1]. Indeed, counterfeit electronic components are increasingly found in the U.S. supply chain. U.S. Customs reports seizure of 5.6 million compromised electronic components between 2007 and 2010, and a Senate Armed Services Committee report documents counterfeit chips found on critical defense systems like the C-130J, C27J, P-8A Poseidon, the night sights for the SH-60B helicopter and mission computers for THAAD missile system. Recycled chips fabricated by hand in Southeast Asian chop shops can fail catastrophically; chips containing malware can be manipulated to crash their host weapons or industrial system.[2]

The second kind of threat comes to us through malware. The weaknesses that malware exploits include configuration errors and vulnerabilities in hardware and software. So called "Zero Day" vulnerabilities apply here. They consist of previously unknown weaknesses in software found by an actor and exploited by him for the first time to compromise or exploit networks.

The third threat vector involves human intervention. One track operates through social engineering, in which an actor does intensive biographical work on a target and develops a message that causes that person to open an attachment which infiltrates controlling software into the target's computer. This vector also includes insider threats, where a trusted person inside the business or institution steals software or data or corrupts them.

[1] David Clark, Thomas Berson, and Herbert S. Lin, Editors, "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," p.75 (Washington, DC, The National Academies Press, 2014).
[2] http://www.homelandsecuritynewswire.com/fake-chips-china-threaten-us-military-systems?page=0,1) "Fake chips from China threaten U.S. military systems" (September 9, 2010); and Senate Committee on Armed Services Report, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain." (May 21, 2012).

Recent reports about harmful mischief in the cyber realm (e.g., Mandiant's "APT1: Exposing One of China's Cyber Espionage Units," and McAfee's Reports entitled "Shady Rat" and "Night Dragon") and what has been disclosed about the persistence and criticality of penetration into the architectures of companies like Google, RSA, and now Target and Michaels, along with the persistent pattern of attempted intrusions into the U.S. banking system, provide insight into the persistent nature of malicious activity and the ephemeral nature of cyber security, stability and privacy.

The growing dependence on the Internet and the capacity of state and non-state actors to misuse, abuse, and exploit technologies to do harm compounds the potential for damage. Symantec's 2013 Security Report documents the rapid growth of threatening behavior on the Internet; some findings in the report indicate:

- 42% increase in targeted attacks in 2012 over 2011.
- 31% of all targeted attacks were aimed at businesses with less than 250 employees. This category of firm, critical to defense R&D cannot afford extensive cyber defenses.
- 32% of all mobile device threats steal information.
- 69% of all e-mail in 2012 was spam.
- The number of phishing sites, those that act like social networking sites, increased 125%.
- Web-based attacks increased 30%.
- 5,291 new vulnerabilities were discovered in 2012, 415 of them on mobile operating systems.[3]

Cyber conflict between nations exploiting any one of the three threat vectors could lead to very severe damage to the integrity of U.S. information architectures. It could damage our ability to communicate, operate, and control escalation, and our ability to preempt attacks. Cyber conflict that integrates measures across all three

[3] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, Internet Security Threat Report 2013: Volume 18, Symantec Corporation.

vectors could have a cascading impact that seriously disrupts and damages U.S. operational and commercial capacity in an unprecedented, idiosyncratic way. The damage could go to the point of making us non-competitive in markets and, in the extreme case, undermining basic national functions embedded in our infrastructure. We are actually seeing very worrying versions of this kind of campaign.

During the development of this report, the ISAB Cyber Study Group met with a number of private sector companies. Based on the compilation of cyber, corporate, and economic data, one such company has determined that nation-state threat actors are conducting anti-trust and economic schemes using cyber intrusion and exploitation as a catalyst for market entry and growth, leading to accumulation of market share. Furthermore, their research revealed that these adversaries have a broad understanding of U.S. industries, processes and systems, internal control weaknesses and the cultural and psychological nuances of the broader markets better than most operational, financial and IT executives within the affected industries. At least 25 industries and 48 companies have had indications of offensive nation-state cyber-economic activity against them within the last five years.

The potential impact of activity like this with simultaneous exploitation along all three of the threat vectors could be enormous. With Russian cyber attacks in Georgia in 2008 and Ukraine in 2014 executed in support of military operations, we have seen the emergence of a new offensive military potential. Attacks on critical infrastructure (which could include our monetary system and our networked electric and water utilities and transportation control facilities) made in support of an offensive military campaign -- or for purely economic, political or other gain (e.g., criminal or terrorist activity) -- could have a devastating effect on U.S. strategic capability. The challenges inherent in the increasingly opaque nature of the dynamic software combinations needed to run large systems and to counter human misbehavior make the defender's job very difficult.

> "The complexity of these scenarios, which results in part from massive inter-connectivity and dependencies between systems that are not always well

understood, has made it difficult to develop a consensus regarding the probable consequences of an attack."[4]

The potential for international relations being destabilized due to cyber activities creates a special concern for the Department of State. The National Academies of Science pointed out that "the world is organized around nation-states and national governments, and every physical artifact of information technology is located *somewhere*. Consequently, one might expect cyberspace-related tensions to arise between nations exercising sovereignty over their national affairs and interacting with other nations."[5] Many scenarios are possible, among them the actions of a third party (nation-state or not) undermining the relations between two countries. For example, in a cyber attack by country A on country C using means in country B, country C might likely mistakenly blame country B, an innocent bystander. To avoid escalation, means must be found to contain the damage and identify the true nature and perpetrator of the attack.

Cyber has a frustrating quality, in that many potential remedies can have negative consequences.[6] Making cyber systems more resistant to attack slows them, cutting into their accessibility, openness, convenience and speed, among other attributes that users value greatly. Pushing for greater capability for attribution impinges on privacy. Norms for state behavior offer a partial solution here. Discussions on norms and compromises needed to make them acceptable offer an opportunity to examine their value and to generate consensus that leads to adoption, which even if only partial, would offer some progress.

Realities:

In addition to the threat environment, other realities bound the art of the possible. Addressing them will help foster international cooperation, which should lead to progress toward greater trust and cyber stability internationally.

[4] Scott Charney, et al, "Rethinking the Cyber Threat, a Framework and Path Forward," Microsoft Corporation, p.6.
[5] Clark, Berson, and Lin, Ibid., p. 11.
[6] Eg., Ibid.

The rhythm of innovation in information technology does not allow for accurate prediction of when and what new capabilities will emerge in two years, let alone five, the horizon used in U.S. fiscal planning. Nor can one predict with certainty unexpected capability developed using tweaks on obsolescent or new technological approaches. Creating and fielding persistent countermeasures remains problematic until one can actually see the products of the next generation emerge in the market or in the field. The arrival of ever newer technological opportunities can, because of the unpredictability of the innovation cycle, create continuing technological surprises that undermine deterrence. If we do not have an agile and aggressive process of innovation, we risk falling behind in development of the critical capabilities and infrastructure that undergird our national security.

Some form of deterrence is necessary to prevent the most extreme attacks using cyber means by nation states and the most capable non-state actors. There are two basic types:

- Deterrence through denial, which involves creating a defense so tough that the expense, time and effort to breach it discourage attack from all but the most capable players. Likewise, "making infrastructures resilient makes them less attractive targets,"[7] contributing to deterrence through denial. Creating a system or infrastructure that is extremely resilient could persuade a potential attacker not to attack, or at least because of quick response replacement systems, make attacking less attractive. For example, a network server, "is not attractive if there is a remote server that can automatically kick in if the main server goes down."[8]

- Conventional deterrence by threat of reprisal, which requires the capability and will to punish an attacker and instill an appreciation of that reality to potential attackers.

However, deterrence overall is less effective with ideologically radical non-state actors who rely weaknesses in commercial technologies for their means of attack

[7] Stephen Flynn, "The Edge of Disaster," p.154 (New York, Random House, 2007).
[8] Ibid. p.99

and who have no prized physical assets that can be threatened by our kinetic or cyber means of response.

Attribution of cyber attacks poses difficult and unique problems. One may not identify an attacker for weeks or months. One may not know initially whether the attacker is a nation state, a non-state group, a lone actor, or initially a hiccup in the system architecture. In its report on Chinese attacks on a small U.S. company, Mandiant, one of the most capable cyber security firms, took months to identify the institution in China that made attacks over a long time, almost bankrupting the firm, which now is cited in Department of Justice indictments of Chinese citizens. Fostering confidence-building measures (CBMs) and norms of behavior accepted by many nations could improve attribution. Locating the attacker quickly would support our national will as well as that of allies in case of a serious attack on the United States. If a prospective attacker believes we can attribute his actions quickly, we may be able to influence his decision to attack or not.

In the international search for remedies to the Hobbesian nature of cyberspace, some entities active in this arena, such as the International Telecommunications Union (ITU) and International Standards Organization (ISO), see the current confusion as an opportunity for their own growth.[9] While international organizations can be useful or even essential, we should make sure that dependence on them does not yield solutions fraught with bureaucratic friction. Hence, we support a two-tier approach for building consensus toward future norms: continued multilateral negotiations along with ongoing efforts to engage bilateral discussions that can, in principle, lead to or at least be compatible with multinational commitments.

Deterrence in Cyberspace:

Deterrence as a best practice plays a crucial role in cyber stability, and requires that we create a fear on the part of the prospective attacker of failed or useless results

[9] Abraham Sofaer, David Clark, and Whitfield Diffie, in "Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy," p. 186 (Washington, DC, The National Academies Press, 2010).

(deterrence by denial), of unacceptable harm or costs to valued capital (deterrence by threat of reprisal) that dissuade a prospective attack, or deterrence based on the resilience of one's architecture (deterrence by resilience). Achieving this capability has clear benefit for protection against critically damaging attacks, and may have some value in preventing lesser incidents. The basis for deciding on a response depends fundamentally on the severity and material physical effects of the attack. At a certain level of damage, destruction and casualties, an attack by cyber means becomes the equivalent of an armed attack, which under international law triggers the right of self-defense.

Prevent and Protect

In the cyber world, in addition to likelihood of response, a modified theory of deterrence requires protection against critically damaging attacks, the ability to stop attacks underway, and assured rapid recovery from them. Proportional response requires attribution. In addition, routinely demonstrating the capability to manage lesser events gives us the ability to discourage escalation as well as to demonstrate capabilities that enhance deterrence. These capabilities would create a high degree of uncertainty in regard to the harm or costs to valued capital we could inflict on a potential attacker. Agreements –formal or informal - on what constitutes the limits between state-sponsored exploitation and armed attack would greatly assist national decisions on redress and response by targeted nations. Specifically, while recognizing that the distinctions between different levels of attack are ultimately political, it would be useful to identify explicit criteria for different levels of attack based on military, economic, social and technical considerations.

A cyber attack may crescendo beyond the original intent of the attacker. In a crisis, discerning intent is critical to effective decision-making about response. In an escalatory situation, identification of decision points becomes vital. Accordingly, to develop our own responses, we need a national effort to implement improved means for reliably attributing the sources of attacks in near real time. Creating and maintaining these capabilities offers crucial support to deterrence itself. This effort will require a more rapid cycle of innovation focused on capabilities to gain effective attribution, enhanced resilience, and identification of

attackers' assets that can be credibly held at risk at an acceptable level of escalation.

Credible defense and offense play a role here. Deterrence of cyber attack depends on a layered architecture, including one in which our weapons of certain response (cyber and kinetic) and the command and control capability both to make accurate assessments and to conduct attribution and response reside in a highly secure and air-gapped strategic core in which all deterrence systems are designed and manufactured in trusted venues and foundries. Capabilities with conventional sensors to assist with attribution would protect second priority systems, most likely conventional military capabilities, infrastructure and key civilian entities. Normal civilian systems would protect the outside layer. The critical requirement here rests in the confidence on our part and that of our adversaries that no matter what the attack, the key functions of government could be sustained and the strategic core would respond proportionally.

Establishing credibility, advocating and implementing transparency, as needed, and understanding potential responses in a crisis are critical prerequisites to defining any deterrence policy that might be used to enhance cyber stability. During a crisis, having the insight and the confidence to assess early in the flow of trigger points when an opponent is "all in" for attack and no longer subject to deterrence offers a critical advantage. These measures will require an unparalleled degree of inter-agency consensus and cooperation that must be reached, instilled and rehearsed before onset of the rush of activities that indicate likelihood of significant attack.

Detect and Contain

Given a good defense, attribution and high confidence in means of response, understanding trigger points for instability in the decision regime of opponents offers a framework for attribution and escalation control. Important clues that will help us to identify and contain the attacker quickly lie in the ramp-up of steps from small precursors that can progress rapidly to the intensity of a "use of force" attack. Such steps can include:

- Precursory activity, perhaps including multiple probes or embedding of malware within a cyber system, but with no immediate impact on functionality: an analog of "preparing the battlefield."
- A cyber event with only minor, though visible, functional effect.
- A cyber attack corresponding to "use of force," as distinct from lesser attack; something like a cyber version of 9-11, which while horrifying did not collapse national systems and infrastructure.
- A cyber attack corresponding in effect to the kind of "armed attack" normally associated with an act of war, one with a rapidly accelerating geographical and severe impact on national capabilities intended to foster chaos and collapse of national will.

The first level of detection, discernment of particular patterns of activity, and containment and prospects of leading on to levels 3 and 4 raise the question of whether there is anything short of an armed attack that could lead to cyber-induced instability. It might be possible for the United States to develop a counter to an attacker's cyber version of "preparing the battlefield" early enough in the cycle to afford us an opportunity for effective defensive action. If detecting the early stages in ramping up to an "armed attack" identifies behaviors that only an attacker makes, seeing the preliminaries offers the first evidence that could lead to attribution and actions to enhance deterrence. For purposes of warning, crisis management or deterrence, how would indices of attack be identified in a manner that is convincing to the United States (both the USG and citizenry), our friends and allies, and our prospective adversaries?

At any level, limiting harm requires immediate defensive action – detection and containment – which can begin at a local level. However, ambiguity pertains in the cyber domain because certain actions do not require attribution yet can be viewed as offensive (e.g., isolating an attacking computer network that is owned by an innocent party but has been taken over by a third party, a malicious botnet, for instance). No commonly accepted set of standards apply in cyberspace, which has uniquely complicating factors that heighten the effects of espionage, surveillance, theft of identities and intellectual property(IP), a reality that hampers decisions on proportional response. But the national decision on whether a given attack crosses

the boundary between exploitation or nuisance and armed attack will depend on a national determination of the degree of damage and casualties inflicted.

Respond and Recover

Once the process of containment of a cyber attack is underway, movement toward response and recovery must begin. Knowledge gained from containment of the attack will provide insights that will suggest the means for countering the attack and begin the process of deciding and acting in response. Quickly gaining that insight is crucial.

The implications for response of the duration, intensity and severity (magnitude) of an event need to be addressed.[10] Events are less actionable, in terms of a response, if they take place over a longer than a shorter time, just as, for different reasons, they are less actionable if they have smaller rather than greater consequences. This pattern has relevance to U.S. concerns over long-term loss of intellectual property (IP). Persistent thefts of small elements of IP over a long time can provide the thief a significant technological advantage in the marketplace. Although the United States draws a distinction between gathering intelligence for national security and gathering information for business and economic interests,[11] international consensus about the operational distinction between intelligence gathering and industrial espionage is elusive. Theft of intellectual property goes on apace.

The differences between use of force and armed attack are important for identifying the types of response consistent with international law. The 15 nations participating in the UN Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013 accepted that international law (to include the Law of Armed Conflict) applies to cyberspace, while acknowledging that there is much room for interpretation and therefore disagreement on some specific issues.

[10] e.g., M. N. Schmitt, in "Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy," pp. 155-156 (Washington, DC, The National Academies Press, 2010).
[11] Clark, Berson, and Lin, Ibid., p.72.

In short, increasing international consensus on the need for stability, norms as guides for best practice, real-time sharing of malware data, pursuit of greater capabilities for attribution of attacks, support of deterrence by denial and by conventional means, and sharing expertise with allies and friends offer important opportunities for enhancing stability.

Recommendations for International Cooperation:

Cooperate on Crime as a First Step: The National Academies of Sciences report highlighted that "When another nation's laws criminalize similar bad activities in cyberspace, the United States and that other nation are more likely to be able to work together to combat hostile cyber operations that cross their national borders."[12] Thus, as a starting point, common areas of cooperation between the United States and as many foreign countries as possible should be established on practices generally held as felonious: cybercrime, child pornography, theft of intellectual property, etc. This consensus can be a step toward stability on the international networks and toward the widespread use of CBMs.

Seek International Consensus on Rules of the Road: In many quarters involving the use of the Internet, the United States is looked upon warily simply because of our significant presence and capability. In our declaratory statements and actions, the United States should advocate rules of the road that improve stability of the Internet through an international understanding that it is a marketplace and commons for the good of all. In international forums focused on cyber, the United States should work to build a shared understanding of how cyber activities can lead to instabilities in relations between countries and how instabilities can be mitigated or avoided altogether by transparency. The United States should seek to gain agreement on normative behaviors in a continuing broad-based effort, and expose attempts to regulate Internet governance and increase control of cyberspace, particularly content, in the name of social control.

[12] Ibid., pp. 57-58.

- The Department of State should continue to build on the consensus of the Third Meeting of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security that international law, and in particular the UN Charter, applies in cyberspace.

- The Department of State should support the effort to buttress sound decision-making in the escalation to and during the impact of armed attack by cyber means by advancing and accelerating efforts to support the development of norms for behavior, leveraging the theory of deterrence adapted to apply to cyberspace, and defining clear objectives for international collaboration which would include real time sharing of data on attacks. Norms might, for example, include ruling attacks on critical infrastructure – whether military (e.g., nuclear command and control systems) or civilian (e.g., electric power grid, financial networks) – as being unacceptable.[13]

- Because of the divergent interests of national players in cyberspace, as well as the political environment in our own domestic national legislature, use of treaties and formal agreements can be problematic. Therefore, wherever possible, the Department of State should encourage the use of agreed upon best practice and consensus norms as boundaries to behavior. This effort depends on a framework and mechanisms for cooperative action in identification of attacks; recovery from them; prevention and pursuit of both state and non-state attackers; and on continuous system improvement internationally. To govern state behavior in cyberspace and to reinforce the emphasis on norms, the Department of State should consider proposing models analogous to the Proliferation Security Initiative (PSI) or the Missile Technology Control Regime (MTCR.)

- Working to define norms and adhering to them offers a way of generating a dialogue that could lead to a generally accepted set of guidelines for

[13] We acknowledge that many details may need to be addressed for such norms to be effective, including definition of what constitutes an attack (from intrusion to partial disruption to full disablement) and the target(s) (in this case, what constitutes "critical infrastructure"), as well as acceptable responses.

behavior. The debate over norms should help the international community to agree on best practice.

Enhance Governments' Situational Awareness through Information Sharing: This element involves real time and, to the extent feasible, automated sharing of cyber risk information (e.g. Internet protocol address/domain names associated with attacks, and malware signatures) between and among nations, their institutions involved in cyber stability, and the private sector. A threat indicator is simply an Internet artifact associated with an attack. The success or failure of the attack does not need to be shared to develop situational awareness within the sharing community. Combining the efforts of academia, business and government, these organizations would retransmit signatures of malware immediately as broadly as possible to allow Internet operators and security officials to evolve their networks to deal with new threats before they go viral. They would create and foster an international framework for trusted preemption, post-attack recovery and reconstitution of disrupted cyber networks and the physical elements of critical national infrastructures.

- Include establishment of multinational cooperative response mechanisms that improve the capabilities of Cyber Emergency Response Teams (CERTs) for the purpose of building relationships, sharing expertise, managing operational risk, and deriving and promulgating lessons learned.

- Develop a framework of priorities for attribution, recovery and reconstitution. Acceptance of this framework would require agreement on activities to share sensitive information about system failures and sufficient transparency to create trust in recovering systems to build confidence to allow rapid reconnection from system to system.

Combat Theft of Intellectual Property: Thefts of small elements of IP accumulated over a long time can provide a significant technological advantage to the thief over the victim, most critically in the build up to and the moment an event transitions into an attack. Given that this phenomenon also applies directly to theft of IP, the Department of State should promote cooperative work to i) understand

how IP theft can cumulatively undermine cyber stability; ii), curb the theft of IP; and iii) manage the effects of cyber-enabled IP theft on international stability.

Expand Education and Capacity Building: The Department of State should develop means to help nations less capable in cyberspace to improve their capability and to adopt best practices. Collaboration and assistance will enhance security and stability of the global cyber infrastructure and foster good will that could provide incentives for any "fence sitting" nations to participate in the effort to limit unacceptable behaviors in cyberspace.

- Countries that have minimal capability for defense may welcome working with public-private partnerships to improve stability in their own networks. Given acceptance of norms of behavior, countries may accept the value in the benefits of widespread sharing of malware signatures and other types of threat information. State should therefore establish programs to improve their capability across the board as a way to enlist them in the effort for greater cyber stability, especially in the acceptance of norms for behavior in cyberspace. Developments in cyber defense offer capabilities (some now available in the commercial marketplace) that can help nations practice Deterrence by Denial. Part of our assistance to nations that have weak capabilities in cyber security would involve an effort to educate national leaders about the need to have in place deployable defenses based on best practice, a benefit for us all.

- To improve the cyber defenses of the less capable nations, sponsor teams of faculty and graduate students in computer science and engineering in spending a summer or other times working with cadre in the crisis response agencies of these nations. This kind of program offers activity not associated with the intelligence community, and would bring CERTs of those nations to a better level of practice.

- Business could also play in this effort. As a priority, sponsor deployment of teams of cyber professionals from the business institutions in Track II communications in this area of training and leader education.

- Foster a program through country teams in which U.S. universities would form exchange post-doctoral fellowships between departments in computer science and engineering in other nations, with the proviso that after their fellowship, students must spend a period working in their own national CERTs.

- Develop senior executive leaders across all sectors of society that have authority over cyber issues by conducting unclassified international cyber exercises, similar to joint and combined military exercises. These activities would allow leaders at the highest national levels to see the typology of attacks, the potential damage that can be caused by them, and the challenges of attribution and response, as well as remedial practices to mitigate them.

- Using the assets of country teams, provide technology grants in support of countries less capable in cyberspace but willing to adopt best practices.

Promote Attribution and Prosecution: Redress depends on agreed upon processes for international cooperation to identify and pursue attackers and criminals by assisting in attribution and where possible, employing legal sanctions based on national and international law. The Department of State should promulgate and incorporate in policy the benefits and dangers of strong authentication technologies and more effective technical trace-back capabilities in the context of more streamlined international assistance.

Leading by Example: The Department of State should promulgate clear and credible norms for cyberspace through public statements articulating U.S. policy in a way that expresses U.S. values in support of international stability. These statements should acknowledge the inherent uncertainties.

- Cyber attacks can have significant unintended consequences. As part of declaratory policy, the United States should state that it will respond to all consequences – including unintended ones, of any cyber attack on the United States or its allies. Effects, not means, will govern our responses.

- Demonstrate that the United States sets rigorous rules of engagement for responding to cyber events through cyber and non-cyber means, whether by technical, diplomatic, financial or military responses.

- Mindful of the threat of strategic cyber attack, the United States, perhaps with a group of nation state partners, should mature, maintain and promulgate a substantiation of deterrence of attacks, and as opportunities arise, extend the umbrella of deterrence to other less capable allied and friendly nations.

Recommendations on How to Engage and Partner with Others:

Initially, we should be able to rely on our traditional allies to cooperate with us in defining and institutionalizing norms for behaviors in cyberspace. Russia and China may continue to try reshaping the international precepts for behavior in cyberspace, both to advantage internal stability and to pursue expansive strategic goals. Russia's use of cyber warfare against both Georgia and Ukraine emphasizes the near certainty that cyber has become a critical capability in preparation for and conduct of any military operation.

At every turn, the Department of State should stress how all nations have a stake in the stability and security of cyberspace, though not at the expense of core international values such as human rights, privacy and legitimate freedom of speech (freedom of speech in cyberspace requires careful consideration in light of many factors, including the capability for authentication of messages and the fact that some speech – incitement to terrorism, for instance – is criminal and should not be protected). These efforts could bring along states with widely different, self-interested rules for Internet use as the consensus matures and expands by demonstrating the benefits of cooperation.

Concrete measures probably will be most achievable initially on a bilateral basis and could be supported by the kind of assistance provided by the teams cited above. In the short term, the Department of State should focus on cyber relationships with countries having concerns and interests congruent with ours.

Bilateral CBMs could then be extended to other countries to create broader coalitions. Global/multilateral discussions through the UN GGE and other existing UN venues should proceed in parallel. Norms and protocols could eventually be linked into coalition agreements. The Additional Protocol to IAEA Safeguards or the Trans-Pacific Partnership may provide models.

Private Sector as a Leader and Enabler: Cooperation can be expected from U.S. influencers and institutions in business and academe, provided that the courses of action taken and the process of developing them include these organizations and conform to their institutional interests and needs. These entities own or provide most of the Internet architecture, its communications means, and with Cloud technology, the means of storing and working with data, as well as widespread research and development efforts. We need U.S. (and multinational) business and academic institutions as involved players. The Department of State should engage the business community in updating and, as needed, forming public-private partnerships that can leverage the diverse expertise of the information and communication technology industries to provide policy and operational and technical expertise to inform, shape, and participate in Department of State efforts. The public-private partnerships should help focus on cyber security as an essential element in economic development and explore how to combine public and private resources such that country teams can help the less capable nations in the cyber realm improve the security of their systems by using best practice.

Public-private partnerships should be utilized to address implications for the business community of U.S. international policies for cyberspace, including their unintended consequences, by including business and academe early on in development of these courses of action.

Conclusion:

The open nature of cyberspace, the access to information it enables, and the creativity that results, encourages a growing potential for a unique and accelerating process of innovation. This process also threatens individual privacy and the function of national infrastructure and financial systems in an historically unprecedented way. As the National Academy of Sciences points out,

"cybersecurity is important to the United States, but the nation has other interests as well, some of which conflict with the imperatives of cybersecurity. It is important to recognize that tradeoffs are inevitable, and the nation's political and policy-making bodies will have to decide on a case-by-case basis which national interests supersede increased cyber security."[14] By encouraging best practice, supporting and promulgating a modified theory of deterrence, and fostering international consensus on conduct in cyberspace among allies and friends, the Department can help in the national effort to allow the greatest utility from cyberspace in ways that do no harm.

[14] Ibid., p. 81.

Appendix A – Summary of Recommendations

Recommendation 1. Cooperate on crime as a first step. As a starting point, common areas of cooperation between the United States and as many foreign countries as possible should be established on practices generally held as felonious: cybercrime, child pornography, theft of intellectual property, etc.

Recommendation 2. Seek international consensus on rules of the road. In our declaratory statements and actions, the United States should advocate rules of the road that improve stability of the Internet through an international understanding that it is a marketplace and commons for the good of all. In international forums focused on cyber, the United States should work to build a shared understanding of how cyber activities can lead to instabilities in relations between countries and how instabilities can be mitigated or avoided altogether by transparency. The United States should seek to gain agreement on normative behaviors in a continuing broad-based effort, and expose attempts to regulate Internet governance and increase control of cyberspace, particularly content, in the name of social control.

- The Department of State should continue to build on the consensus of the Third Meeting of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security that international law, and in particular the UN Charter, applies in cyberspace.

- The Department of State should support the effort to buttress sound decision-making in the escalation to and during the impact of armed attack by cyber means by advancing and accelerating efforts to support the development of norms for behavior, leveraging the theory of deterrence adapted to apply to cyberspace, and defining clear objectives for international collaboration which would include real time sharing of data on attacks.

- Wherever possible, the Department of State should encourage the use of agreed upon best practice and consensus norms as boundaries to behavior. To govern state behavior in cyberspace and to reinforce the emphasis on norms, the Department of State should consider proposing models analogous

to the Proliferation Security Initiative (PSI) or the Missile Technology Control Regime (MTCR.)

Recommendation 3. Enhance governments' situational awareness through information sharing. Enhancing current capabilities of USG organizations in sharing of threat indicators across national boundaries would offer one step. Combining the efforts of academia, business and government, these organizations would retransmit signatures of malware immediately as broadly as possible to allow Internet operators and security officials to evolve their networks to deal with new threats before they go viral. They would create and foster an international framework for trusted preemption, post-attack recovery and reconstitution of disrupted cyber networks and the physical elements of critical national infrastructures.

Recommendation 4. Combat theft of intellectual property (IP). The Department of State should promote cooperative work to i) understand how IP theft can cumulatively undermine cyber stability; ii) curb the theft of IP; and iii) manage the effects of cyber-enabled IP theft on international stability.

Recommendation 5. Expand education and capacity-building. The Department of State should develop means to help nations less capable in cyberspace to improve their capability and to adopt best practices.

- State should establish public-private partnership programs to assist countries that have minimal capability for defense to improve stability in their own networks, as a way to enlist them in the effort for greater cyber stability, especially in the acceptance of norms for behavior in cyberspace. Part of our assistance to nations that have weak capabilities in cyber security would involve an effort to educate national leaders about the need to have in place deployable defenses based on best practice.

- To improve the cyber defenses of the less capable nations, sponsor teams of faculty and graduate students in computer science and engineering in spending a summer or other times working with cadre in the crisis response agencies of these nations.

- As a priority, sponsor deployment of teams of cyber professionals from the business institutions in Track II communications in this area of training and leader education.

- Foster a program through country teams in which U.S. universities would form exchange post-doctoral fellowships between departments in computer science and engineering in other nations, with the proviso that after their fellowship, students must spend a period working in their own national CERTs.

- Develop senior executive leaders across all sectors of society that have authority over cyber issues by conducting unclassified international cyber exercises, similar to joint and combined military exercises.

- Using the assets of Country Teams, provide technology grants in support of countries less capable in cyberspace but willing to adopt best practices.

Recommendation 6. Promote attribution and prosecution. The Department of State should promulgate and incorporate in policy the benefits and dangers of strong authentication technologies and more effective technical trace-back capabilities in the context of more streamlined international assistance.

Recommendation 7. Lead by example. The Department of State should promulgate clear and credible norms for cyberspace through public statements articulating U.S. policy in a way that expresses U.S. values in support of international stability. These statements should acknowledge the inherent uncertainties and vulnerabilities.

- As part of declaratory policy, the United States should state that it will respond to all consequences – including unintended ones, of any cyber attack on the United States or its allies. Effects, not means, will govern our responses.

- Demonstrate that the United States sets rigorous rules of engagement for responding to cyber events through cyber and non-cyber means, whether by technical, diplomatic, financial or military responses.

- Mindful of the threat of strategic cyber attack, the United States, perhaps with a group of nation state partners, should mature, maintain and promulgate a substantiation of deterrence of attacks, and as opportunities arise, extend the umbrella of deterrence to other less capable allied and friendly nations.

Recommendation 8. Adopt a two-tier approach for building consensus toward future norms: continued multilateral negotiations along with ongoing efforts to engage bilateral discussions that can, in principle, lead to or at least be compatible with multinational commitments. In the short term, the Department of State should focus on cyber relationships with countries having concerns and interests congruent with ours. Bilateral CBMs could then be extended to other countries to create broader coalitions. Global/multilateral discussions through the UN GGE and other existing UN venues should proceed in parallel. Norms and protocols could eventually be linked into small coalition agreements. The Additional Protocol to IAEA Safeguards or the Trans-Pacific Partnership may provide models.

Recommendation 9. The Department of State should engage the business community in updating, and as needed, forming public-private partnerships that can leverage the diverse expertise of the information and communication technology industries to provide policy and operational and technical expertise to inform, shape, and participate in Department of State efforts. The public-private partnerships should help focus on cyber security as an essential element in economic development and explore how to combine public and private resources such that country teams can help the less capable nations in the cyber realm improve the security of their systems using best practice. Such partnerships should be utilized to address implications for the business community of U.S. international policies for cyberspace, including their unintended consequences, by including business and academe early on in development of these courses of action.

Appendix B – Definitions

Cyber attack: In order to influence political will of the target or to enhance capability of the attacker, an act in cyberspace to disrupt or damage control systems or major infrastructure or a network in order to inflict a severe loss on the targeted nation's economy, military capability, well being of the populace, and continuity of government. Cyber attacks would include an "armed attack" as described in the discussion of deterrence and trigger points; one with effects that equate to an act of war.

Cyber Deterrence: Taking actions or adopting a policy to prevent, or at least discourage, other actors from attacking the cyber resources of a state. Cyber deterrence contains many aspects of traditional deterrence and considers:

- Possession of the demonstrated capability (attribution + attack means) and will to inflict unacceptable costs on the valued physical capital of an adversary, convincing him not to attack.

- In the case of non-state actors and terrorists, who have no capital to threaten and an ideological preference for the spectacle of martyrdom or satisfaction in creating shocking events, Deterrence by Denial involving defenses that take extensive effort and cost to breach and that in the process potentially lead to arrest or other legal sanction may have significant expected utility.

Cyber Security: Organizational actions that provide assurance of legal and reliable use of cyberspace, from hardware and software systems to operations and information (data), so that it is protected and usable in the manner expected by its originators and recipients.

Cyber Stability: An environment where all participants, including nation-states, non-governmental organizations, commercial enterprises, and individuals, can positively and dependably enjoy the benefits of cyberspace; where there are benefits to cooperation and to avoidance of conflict, and where there are disincentives for these actors to engage in malicious cyber activity.

In a crisis during an attack or even before attack, cyber stability depends fundamentally on transparency and the knowledge on both sides of their opponent's trigger points, that is, actions that lead to escalatory decisions, and likely inexorably to deployment of more powerful capabilities and on to full spectrum conflict. Fostering transparency, attribution, and the political will to act provide the critical underpinnings of cyber stability.

Cyber Terrorism: An idiosyncratic attempt using cyber means by a non-state actor to generate fear or widespread shock and panic to affect political or economic decisions of a nation-state.

Malicious [*criminal*] cyber activity: Offensive cyber activity that violates the law of the affected state, international law, the conventions of the United Nations or norms promulgated by international authority. This kind of behavior would include theft of intellectual property, disruption or damage to information systems and their content, or destruction of national infrastructure, either as a nuisance or a national emergency.

Trust: High confidence among players that each will adhere to rules of the road agreed to as either international norms, conventions, law or consensus best practice that the Internet will function reliably.

Appendix C – Terms of Reference

UNDER SECRETARY OF STATE FOR
ARMS CONTROL AND INTERNATIONAL SECURITY
WASHINGTON

July 17, 2013

MEMORANDUM FOR THE CHAIRMAN, INTERNATIONAL SECURITY ADVISORY BOARD (ISAB)

SUBJECT: Terms of Reference – ISAB Study on a Framework for International Cyber Stability

The International Security Advisory Board (ISAB) is requested to undertake a study of a potential architecture for enhanced international cooperation in promoting a peaceful, secure, and open cyberspace environment.

Malicious activities in cyberspace are becoming more frequent, sophisticated and costly in the damage they inflict on governments, business, and society. While the United States seeks to retain the openness of the Internet, its efforts to achieve a global common understanding of the norms of acceptable state behavior in cyberspace face resistance from countries that desire to regulate Internet governance and increase state control of cyberspace, including its content, in the name of security. In seeking solutions to transnational cybersecurity issues, an alternative to a "one-world" strategy developed and carried out by all actors is a coalition of like-minded states that affirm common norms of state behavior and cooperate to build confidence and capacity in the cybersecurity realm. A third option is developing regional mechanisms and organizations to accomplish these goals.

It would be of great assistance if the ISAB could examine and assess:

- the pros and cons of different strategies for pursuing international cyber stability: particularly global, like-minded coalition, and regional organization approaches;
- how groups of countries could be organized, and how they could operate to promote cyber stability goals;
- what principles, norms and commitments should guide states that work together to promote cyber stability;

- what cyber stability approaches, including confidence-building measures (CBMs), would be most attractive to persuade other states to cooperate;
- how to deal with different cybersecurity priorities among states;
- possible incentives for state restraint from and disincentives to engagement in cyber warfare (sometimes called "cyber deterrence") and options for responding to malicious cyber acts.

During its conduct of the study, the ISAB, as it deems necessary, may expand on the tasks listed above. I request that you complete the study in 270 days. Completed work should be submitted to the ISAB Executive Directorate no later than April 2014.

The Under Secretary of State for Arms Control and International Security will sponsor the study. The Assistant Secretary of State for Arms Control, Verification and Compliance will support the study. Jane Purcell will serve as the Executive Secretary for the study and Chris Herrick will represent the ISAB Executive Directorate.

The study will be conducted in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act." If the ISAB establishes a working group to assist in its study, the working group must present its report of findings to the full ISAB for consideration in a formal meeting, prior to presenting the report or findings to the Department.

Rose E. Gottemoeller

Appendix D – Members and Project Staff

Board Members

Hon. Gary Hart (Chairman)
Hon. Charles B. Curtis (Vice Chairman)

Hon. Graham Allison
Dr. Michael Anastasio
Hon. Douglas Bereuter
Dr. Bruce Blair
Amb. Linton F. Brooks
Brig. Gen. Stephen A. Cheney (USMC, Ret.)
Mr. Joseph Cirincione
Amb. Robert Gallucci
Hon. Sherri Goodman
Amb. Robert E. Hunter
Hon. Shirley Ann Jackson
Dr. Raymond Jeanloz
Dr. David A. Kay
Gen. Lester L. Lyles (USAF, Ret.)
Gen. Montgomery C. Meigs (USA, Ret.)
Rep. Harold P. Naughton Jr.
Hon. William Perry
Mr. Robert N. Rose
Lt. Gen. Brent Scowcroft (USAF, Ret.)
Hon. Walter Slocombe
Dr. James A. Tegnelia
Hon. William H. Tobey
Dr. Joan B. Woodard

Study Group Members

Gen. Montgomery C. Meigs (USA, Ret.) (Chairman)
Hon. Charles B. Curtis
Hon. Shirley Ann Jackson
Dr. Raymond Jeanloz
Gen. Lester L. Lyles (USAF, Ret.)
Mr. Robert Rose
Dr. Joan Woodard

Project Staff

Mr. Richard W. Hartman II
Executive Director, ISAB

Ms. Jane E. Purcell
Executive Secretary

Mr. Christopher Herrick
Deputy Executive Director, ISAB

Ms. Thelma Jenkins-Anthony, ISAB Action Officer

Lt. Col. Erick J. Castro (USAF)
Executive Secretary

This page intentionally blank

Appendix E – Individuals Consulted by the Study Group

	August 28, 2013
Mr. Alfred Berkeley III	Former President of NASDAQ
Assigned Briefers	State Department's Bureau of Intelligence and Research--Cyber Office; the National Security Agency
Mr. Tony Foley	Director, Office of Counterproliferation Initiatives, ISN Bureau, Dept. of State
	September 18, 2013
Mr. Gary Gagnon	Corporate Security Officer, MITRE Corp
Ms. Betty Shave	Assistant Deputy Chief for International Computer Crime, Department of Justice
Mr. Thomas Dukes	Office of the Cyber Coordinator, Dept. of State
Ms. Michelle Markoff	Office of the Cyber Coordinator, Dept. of State
	November 15, 2013
Mr. Drew Morin	Senior Vice President and Chief Technology Officer (CTO), TeleCommunication Systems, Inc.
Mr. Tony Cole	Vice President and Global Government CTO, FireEye, Inc.
Mr. Belisario Contreras	Manager, Cyber Security Program, Organization of American States
Ms. Julie Zoller	Senior Deputy U.S. Coordinator for International Communications and Information Policy, Dept. of State

Mr. John Albert	Office of Conventional Arms Threat Reduction, Dept. of State
Mr. James Lewis	Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies
	March 12, 2014
Ms. Angela McKay	Microsoft Principal Security Strategist
	April 1, 2014
Mr. Brandon Ahrens	Ernst & Young, Advisory Services, Government & Public Sector
Mr. Jeffrey Johnson	Ernst & Young, Advisory Services, Government & Public Sector
Mr. Kevin Nagel	Ernst & Young, Advisory Services, Government & Public Sector